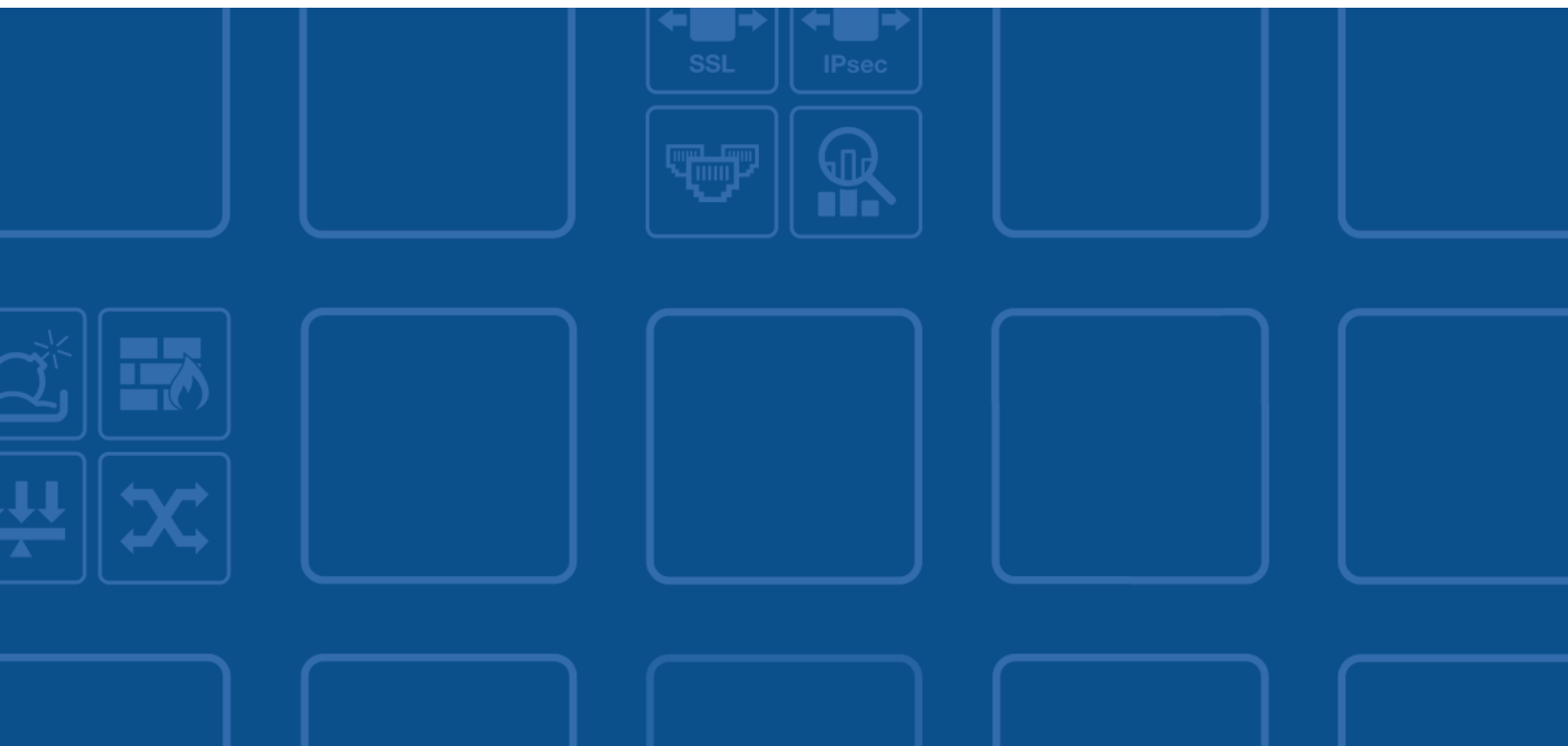
FORTINET
High Performance Network Security

FortiAnalyzer
Report Performance Troubleshooting Guide

Version 5.4.0



FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

July 19, 2018
FortiAnalyzer 5.4.0 Report Performance Troubleshooting Guide
05-540-423043-20180719

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-08-04	Initial release.
2018-03-07	Added *Check Report and Chart Settings* section.
2018-07-19	Added *FortiAnalyzer Report Technology* section.

Overview

This guide helps you to understand FortiAnalyzer report technology and to troubleshoot reporting and FortiView related performance issues. Some troubleshooting steps use CLI commands and require interpreting the results to determine the cause of performance issues.

If your system has reporting and FortiView related performance issues, the following are the most common causes:

- One of the most common causes of report performance issues is overloaded hardware, especially when using VMs. If the hardware is overloaded, changing software configurations can only give minimal performance improvements. To check if the hardware is overloaded, see System Performance on page 8 and Check hardware and software status on page 10.
- If you regularly run a group of similar reports, put them into a group. Grouping reports can significantly improve performance and reduce report generation time. See Group reports on page 11.
- The report diagnostic log gives a lot of information about your reporting process. Check the report diagnostic log and try to determine the cause of report performance issues. See Check Report Diagnostic log on page 7.

This guide also lists other troubleshooting commands and suggested solutions for improving report performance.

FortiAnalyzer Report Technology

Changing some FortiAnalyzer report parameters might require rebuilding the report cache. Depending on the FortiAnalyzer model, your report parameters, and other factors, rebuilding the report cache might cause reports to take a long time to complete. The following are some report parameters that might require rebuilding the report cache (the hcache tables).

- Adding or changing most report filters in the *Filters* section usually require rebuilding the report cache.
- Changing *Devices* from *All Devices* to specific devices.

  Specifying devices adds a filter which requires rebuilding the cache. If you regularly generate reports for specific devices, put those reports into a group.
- Changing the *Time Period* might require rebuilding the report cache depending on the change; even if you are changing from a long time period to a short time period. The *All Reports* > *Cache Status* column shows if a report cache is rebuilding.

Sample report run time

The following table shows the approximate run time for a sample report on different FortiAnalyzer models. Report run time depends on many factors and this table shows some examples of roughly how long a report takes on different FortiAnalyzer models with different log rates.

FortiAnalyzer Model	Report Template	Time Period	Average Log Rate	Run Time Without Cache	Run Time With Cache
FortiAnalyzer 3000F	Security Analysis	1 Day	6000 logs/sec	~ 31 minutes	~ 20 seconds
FortiAnalyzer 2000E	Security Analysis	1 Day	2000 logs/sec	~ 8 minutes	~ 20 seconds
FortiAnalyzer 300F	Security Analysis	1 Day	4300 logs/sec	~ 1 hour 8 minutes	~ 1 minute
FortiAnalyzer VM64 with 2 CPUs and 4 GB memory	Security Analysis	1 Day	350 logs/sec	~ 12 minutes	~ 20 seconds

Troubleshooting Report Performance Issues

Check Report Diagnostic log

For reports that take a long time to run, check the report diagnostic log to troubleshoot performance issues.

To retrieve a report diagnostic log, go to *Reports* > *Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer. Use a text editor to open the log and check the log for possible causes of performance issues.

Following are parts of a sample report diagnostic log and what to look for when troubleshooting report performance.

```
NAME  SCHEDULED  AUTO-CACHE  REPORT GROUP  REPORT TITLE
================================================================================
1     V          V           -             Security Analysis

per-device option: disable
hostname-resolve: disable

Report Status
   Max pending rpts: 100000
   Current pendings: 0
   Max running rpts: 10
   Current runnings: 2
```

Section	What to look for
NAME / SCHEDULED / AUTO-CACHE / REPORT GROUP / REPORT TITLE	Check the `SCHEDULED`, `AUTO-CACHE`, and `REPORT GROUP` columns. • Schedule the reports that run regularly. To configure report schedules, see *Scheduling reports* in the *FortiAnalyzer Administration Guide*. • Enable auto-cache for reports that run regularly, especially schedule reports. See *How auto-cache works* and *Enabling auto-cache* in the *FortiAnalyzer Administration Guide*. • Group reports that run regularly. To group reports, see *Grouping reports* in the *FortiAnalyzer Administration Guide*.
`hostname-resolve`	Ensure `hostname-resolve` is set to `disable`. Resolving hostnames usually takes a long time. If the DNS server is slow or does not support reverse DNS, report generation might hang.

```
Total Quota Summary:
   Total Quota  Allocated  Available  Allocate%
   27201.3GB    1024.0GB   26177.3GB  3.8 %

System Storage Summary:
   Total        Used       Available  Use%
   27501.3GB    1117.6GB   26383.6GB  4.1 %

----------------------------------------
System Performance
Fri Aug 25 12:00:02 2017
----------------------------------------
CPU
   Used:  34.4%
   Used(Excluded NICE):  34.4%
Memory
   Total:  34939888 KB
   Used 23899636 KB 68.4%
Hard Disk
   Total:  28837161872 KB
   Used:  11171927688 KB 38.7%
   IoStat:
Log Rate
   logs/sec: 20326.8, logs/30sec: 20395.6, logs/60sec: 20274.2
Message Rate
   msgs/sec: 3057.4, msgs/30sec: 3068.1, msgs/60sec: 3039.1
```

Section	What to look for
Total Quota Summary and **System Storage Summary**	• Ensure there is enough disk quota and disk space for logging and reporting. Insufficient disk quota might affect report accuracy. Disk quota must be big enough so that quota enforcement does not affect logs used for reporting. If quota enforcement trims the logs or tables used for the reporting period, there might be empty charts or incorrect data.
System Performance	• Check that there is enough system resources including CPU, memory, and disk space. • Check that the log rate and message rate is not so high that it slow report generation. • If the log rate is higher than the sustained rates for your FortiAnalyzer model, the hardware is overloaded and needs an upgrade. The sustained rates for FortiAnalyzer models are listed in the Data Sheet on the FortiAnalyzer web page.

```
----------------------------------------
Run Report
Fri Aug 25 12:00:03 2017
----------------------------------------
[12:00:03] Request hcaches for 9 log tables
chart Traffic-Bandwidth-Summary-Day-Of-Month done, 1 subqrys
   1/1 took 17.88s, 0 hcaches ready, 2 hcaches requested
   overall time used 18.13s
chart Session-Summary-Day-Of-Month done, 1 subqrys
   1/1 took 15.54s, 0 hcaches ready, 2 hcaches requested
   overall time used 15.80s
chart Traffic-History-By-Active-User done, 1 subqrys
   1/1 took 12.79s, 0 hcaches ready, 2 hcaches requested
   overall time used 13.07s
chart Top-Attack-Victim done, 1 subqrys
   1/1 took 1.71s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.71s
chart Top-Attack-Source done, 1 subqrys
   1/1 took 1.51s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.51s
chart Top-Attacks-Detected done, 1 subqrys
   1/1 took 1.91s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.94s
…
…
…
chart System-Summary-By-Severity done, 1 subqrys
   1/1 took 1.22s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.22s
chart System-Critical-Severity-Events done, 1 subqrys
   1/1 took 1.18s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.18s
chart System-High-Severity-Events done, 1 subqrys
   1/1 took 0.46s, 0 hcaches ready, 1 hcaches requested
   overall time used 0.46s
```

Section	What to look for
Run Report	• Check the number of log tables. • Check the number of hcaches requested vs ready. If many hcaches are not ready, then those charts will take a long time. If the number of log tables is high but the number of hcaches ready is low, retrieve the diagnostic log after five minutes. A change in the number of hcaches ready means the report is still running. Since the diagnostic log is updated every five minutes, you can check this log to view reporting progress. • Check which charts take a long time to generate and reconfigure those charts to improve performance.

```
----------------------------------------
Report Summary
Fri Aug 25 12:00:56 2017
----------------------------------------
Number of charts: 58
Number of tables: 9
Number of hcaches requested: 109

HCACHE building time: 53.32s
Rendering time: 13.33s
Total time: 1m7.67s
```

Section	What to look for
Report Summary	• Check the number of hcaches requested, hcache building time, and rendering time. The `number of hcaches requested` = number of charts per report * number of master tables * number of reports.

Check hardware and software status

get system status

This command shows the system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format.

Use this information to check if the hardware is overloaded. This information also helps you and customer support to quickly identify any issues and narrow down the investigation.

Following is a sample result of running this command.

```
Platform Type : FAZ3500E
Platform Full Name : FortiAnalyzer-3500E
Version : v5.4.3-build1187 170517 (GA)
Serial Number : FL99999999999999
BIOS version : 00010001
System Part-Number : P15168-01
Hostname : SAMPLEFZ350
Max Number of Admin Domains : 4000
Admin Domain Configuration : Disabled
FIPS Mode : Disabled
Branch Point : 738
Release Version Information : GA
Current Time : Tue May 23 10:22:53 PST 2017
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 17020.10GB, Total 40314.71GB
File System : Ext4
```

Line	Notes
`Current Time`	This is the SQL insert start time.
`File System`	Ensure the file system is `Ext4`. Other file systems will likely cause performance issues.

What to look for

- Check the hardware `Platform Type`. Consider upgrading older hardware, especially older hardware running newer software such as 5.2 or later.
- `Version` shows the software version. Ensure you are running the latest software version with the newest report engine.
- Ensure `File System` is `Ext4`. Other file systems will likely cause performance issues.

diagnose fortilogd lograte

This command shows the log receive rate.

Following is a sample result of running this command.

```
logs/sec: 121091.0, logs/30sec: 119613.9, logs/60sec: 116695.8
```

What to look for

- If the log rate is higher than the sustained rates for your FortiAnalyzer model, the hardware is overloaded and needs an upgrade. The sustained rates for FortiAnalyzer models are listed in the Data Sheet on the FortiAnalyzer web page.

Group reports

For reports that you run regularly, set up the following:

- Put those reports into a group.
- Schedule those reports. If possible, schedule reports to run at off-peak hours and do not schedule reports to run at the same time as log maintenance tasks.
- Enable auto-cache for those reports.

Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-hcache* completion time.
- Improve report performance and reduce report completion time.

Consider grouping reports in these conditions:

- If you use the same or a similar report template for different FortiGates in the same ADOM.
- If you regularly use different filters on your reports.

Other ways to improve report performance include:

- Avoid running reports at the same time as log aggregation or log transfer.
- Avoid queries to external sources such as DNS (for name resolution) or LDAP (for obtaining a user list).

What to look for

- To check which reports are in a group, see Check Report Diagnostic log on page 7.
- To group reports, see *Grouping reports* in the *FortiAnalyzer Administration Guide*.
- To schedule reports, see *Scheduling reports* in the *FortiAnalyzer Administration Guide*.

Check data policy and log storage policy

Check that the data policy and log storage policy are configured properly for each ADOM in each FortiAnalyzer unit. The data policy specifies how long to keep logs. The log storage policy affects logs and the SQL database. For details, see the *FortiAnalyzer Administration Guide*.

Check report and chart settings

Resolving hostnames usually takes a long time. If the DNS server is slow or does not support reverse DNS, report generation might hang. Check that `Resolve Hostname` is disabled:

- In *Reports Settings tab > Advanced Settings*, check that `Resolve Hostname` is not selected.
- In the *Chart Library*, check that `Resolve Hostname` is set to `Disabled`.

If you do not need to show all results, specify a lower maximum number of entries:

- In the *Chart Library*, check that the chart's `Show Top (0 for all results)` is not set too high. Setting this field to `0` for all results causes FortiAnalyzer to list all logs for the chart.

Check and adjust report auto-cache daemon

get system performance

This command shows system performance statistics such as CPU, memory, and I/O usage.

Following is a sample result of running this command.

```
CPU:
   Used:                 49.51%
   Used(Excluded NICE):  49.51%
        %used  %user  %nice  %sys  %idle %iowait  %irq %softirq
   CPU0 27.89  20.60   0.00  5.40  96.42   0.80   0.00     1.79
   CPU1 21.62  12.61   0.00  8.20  98.38   0.40   0.00     0.40
```

```
Memory:
   Total:  6,134,200 KB
   Used:   3,770,260 KB   61.5%
Hard Disk:
   Total:   82,434,736 KB
   Used:    65,283,648 KB  79.2%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            4.7   0.2   4.4   27.5  144.2   0.2    52.5     8.4   3.9    599578.78
Flash Disk:
   Total:   499,656 KB
   Used:    314,416 KB     62.9%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            0.0   0.0   0.0    0.0    0.0   0.0    13.6     4.6   0.0    599578.78
```

Following is a sample result of high `%iowait`. To see the `iowait` usage and limit, first enable debug messages for SQL commands (`diagnose debug enable`) and set the debug level (`diagnose debug application sqlrptcached 8`).

```
FAZVM64 # [530] iowait usage (27.5%) is over limit (23%).
[530] iowait usage (25.9%) is over limit (23%).
[530] iowait usage (28.3%) is over limit (23%).
```

What to look for

- Check the `Used` and `IOStat` lines to see if I/O is busy.
- If both CPU `%used` and `%iowait` are high, check if the report cache daemon is running:
  ```
  diagnose debug enable
  diagnose debug application sqlrptcached 8
  ```
- If `iowait` is over the limit, cache building (by `sqlrptcached`) will be paused until `iowait` drops below the limit. In this case, do one or both of the following:
  - Change the report schedule to run at a less busy time. To see scheduled reports, run `execute sql-report list-schedule <ADOM>`. To configure report schedules, see *Scheduling reports* in the *FortiAnalyzer Administration Guide*.
  - Enable `aggressive-schedule` so the report auto-cache daemon does not stop even under heavy system load:
    ```
    config system report auto-cache
       set aggressive-schedule enable
    end
    ```

Check and adjust report hcache

diagnose test application sqlrptcached 2

This command shows if hcache creation is able to catch up.

Following is a sample result of running this command.

```
Number of log table read: all=6453(fortiview=0, rpt=6453) pending=1
Number of log table done: all=6453(fortiview=0, rpt=6453) rpt=6453
Current hcache table entries: 155750
```

```
Number of hcache requests sent: 70999
Number of log table vacuums: 39401, pending=2
FortiView hcache load: rounds=817, tbl=653600
ncmdb:
cache hit: sch=0, config=27, chart=140, macro=0, dataset=140 config=27
calls : sch=130, config=11, chart=23, macro=0, dataset=23
```

The following table provides notes about some output lines in the example.

Line	Notes
`Number of log table read`	`pending`=0 means hcache creation is able to catch up. If `pending` is above 0, see What to look for below.
`Number of log table done`	The number of master tables used to calculate the `Number of hcache requests sent`.
`Current hcache table entries`	Total hcache on the system.
`Number of hcache requests sent`	The number of charts per report * the number of master tables * the number of reports.
`Number of log table vacuums`	The postgres built-in status. A `pending` number above 0 indicates insufficient postgres resources.
`FortiView hcache load`	`rounds` is the number of FortiView caches proactively loaded into memory.
`ncmdb`	Report configuration database.
`cache hit`	`config` is the number of enabled auto cache.

What to look for

- In `Number of log table read`, if the `pending` number is continuously above 0 or is increasing, that indicates there are too many pending log tables to read and the system lacks resources to create cache. In this case, consider disabling auto-cache on some reports. See *Enabling auto-cache* and *Reports Settings tab* in the *FortiAnalyzer Administration Guide*.
- Run `execute sql-report list-schedule <ADOM>` and check if there are too many scheduled reports and if auto-cache is enabled. See *Scheduling reports* and *Enabling auto-cache* in the *FortiAnalyzer Administration Guide*.
- Run `execute top` to check which applications are using the most system resources.

execute sql-report hcache-check <ADOM> <schedule-id>

This command shows a specific report's hcache status.

If necessary, check the hcache status of a specific report that you think might be a problem.

For example, if the `ADOM` is `root` and `schedule-id` is `10004`, then run `execute sql-report hcache-check root 10004`.

To get the `schedule-id`, run `execute sql-report list-schedule root` and see the `NAME` column.

Following is a sample result of running the `execute sql-report hcache-check <ADOM> <schedule-id>` command.

```
layout_num:1
start [0] get layout-id:10004.
start report_process, layout-id:10004, layout title:Admin and System Events Report.
device list:All_FortiGates.
reports num:1.


device list[0].FWF60C3G13006291[root].
device list[1].FG3K2C3Z11800039[root].
......


> checking (10004_t10004-Admin and System Events Report) ...
checking chart Admin-Login-Summary...
8/8 (100%) done 0.131 secs used.
checking chart Admin-Login-Summary-By-Date...
8/8 (100%) done 0.128 secs used.
...
```

What to look for

- If a few reports are causing a bottleneck, check those reports' diagnostic log and consider reconfiguring those reports. See also Check and adjust report auto-cache daemon on page 12 and Check and adjust report hcache on page 13.

Report performance troubleshooting commands

The following is a summary of CLI commands for troubleshooting report performance.

CLI	Description
`diagnose debug application sqlrptcached 8`	Set the debug level of the SQL report cache daemon.
`diagnose debug crashlog read`	Print information of all crashed daemons. If daemons crash frequently, contact customer support for assistance.
`diagnose debug disable`	Disable debug message.
`diagnose debug enable`	Enable debug messages to run SQL diagnostic commands.
`diagnose fortilogd lograte`	Show the log receive rate.
`diagnose fortilogd msgrate`	Show message receive rate. One message might contain multiple logs.

CLI	Description
`diagnose log device`	Show disk quota for all logging devices.
`diagnose report status`	Show the maximum number of pending and running reports, and the current number of pending and running reports.
`diagnose test application sqlrptcached 2`	Show if hcache creation is able to catch up.
`diagnose sql show hcache-size`	Show the hcache size.
`diagnose sql status run-sql-rpt`	List the number of log tables, hcaches, and the time to generate each chart in the report.
`diagnose sql status sqlreportd`	Show SQL query connections and hcache status.
`execute sql-report hcache-check <ADOM> <schedule-id>`	Show a specific report's hcache status.
`execuate sql-report list-schedule <ADOM>`	Show a summary table of all configured reports with their configuration status.
`execuate top`	List the processes running on the FortiAnalyzer system.
`get system performance`	Show system performance statistics such as CPU, memory, and I/O usage.
`get system status`	Show the system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format. Use this information to check if the hardware is overloaded. This information also helps you and customer support to quickly identify any issues and narrow down the investigation. • Ensure `Version` is the latest software version. • Check the hardware `Platform Type`. Consider upgrading older hardware, especially older hardware running newer software such as 5.2 or later. • Ensure `File System` is `Ext4`. Other file systems will likely cause performance issues.

`show system report auto-cache`	Show non-default settings in the report auto-cache.
	Ensure auto-cache is enabled by running these commands:
	`config system report auto-cache`
	`  set status enable`
	`end`

FORTINET®

High Performance Network Security